

Building a More Secure and Prosperous Texas

A Report from the
TEXAS CYBERSECURITY, EDUCATION, AND
ECONOMIC DEVELOPMENT COUNCIL

Updated Version

December 1, 2012



About the

Texas Cybersecurity, Education, and Economic Development Council

In 2011, the 82nd Texas Legislature passed and the Governor signed Senate Bill 988, which authorized the creation of the Cybersecurity, Education, and Economic Development Council. The legislation directed the Department of Information Resources to appoint a nine-member council from across government, academia, and industry. The Council is to provide recommendations to the Texas Legislature regarding ways to 1) improve the infrastructure of the state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cybersecurity as an industry in Texas.

Contents

Executive Summary	1
Introduction	3
Texas Economy and Critical Technology Infrastructures at Risk	3
The Texas Cyber Environment Today	3
Looking Back: SIPAC Assessment of Texas Critical Infrastructure	4
Senate Bill 988 Charge and Council Analysis and Assessment	4
Strengths	5
Weaknesses	5
Opportunities	6
Threats.....	6
Council Call for Action.....	6
Findings and Recommendations.....	9
Advancing Cyber Secure Infrastructure in Texas	9
Findings	9
Recommendations	11
Infrastructure Summary	15
Developing the Cybersecurity Industry in the State	15
Findings	15
Recommendations	18
Industry Summary	20
Creating an Enduring Cybersecurity Culture.....	21
Findings	21
Recommendations	21
Education Summary	23
Next Steps.....	25
Conclusion.....	27
Acknowledgements	29
Appendix A: SB 988 Tasking.....	31
Appendix B: Council Membership	33
Appendix C: Glossary.....	35
Appendix D: Business Executives for Texas Security (BETS) Concept	39
Background and Purpose	39
Organization and Structure.....	39

Appendix E: Cyber Star Program	41
General Concept	41
Objective	41
Key Suggestions.....	41
Appendix F: Community Cyber Security Maturity Model.....	43
Appendix G: Report Information Gathering Efforts	51
Appendix H: Examples of Cybersecurity Incidents	53
Appendix I: Resources and References	57

Executive Summary

With the advancement of technology and the proliferation of computer systems and networks, cybersecurity threats to Texas government and industries are evolving in complexity and severity and growing in number, outpacing Texas organizations' ability to protect the state's cyber environment. This puts the private information of Texas citizens, including that of children, at risk. Additionally, the risk extends to the intellectual property of Texas businesses and to the security of the state.

In fiscal year 2011, the 82nd Texas Legislature passed and the Governor signed Senate Bill (SB) 988, which authorized the creation of the Texas Cybersecurity, Education, and Economic Development Council (Council). The Council was chartered to provide recommendations to the state leadership regarding ways to 1) improve the infrastructure of the state's cybersecurity operations, both with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cybersecurity as an industry in the state.

The Council examined three areas of importance to the state: its cybersecurity infrastructure, its cybersecurity industry, and the cybersecurity educational needs for fostering a vigilant and effective cyber culture. A detailed discussion of these areas is provided later in this document. As a result of the examination, the Council found that Texas must establish a statewide focus for its cyber environment. This focus would include Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens and to spur innovation in the cyber environment. The Council recommends:

- 1. Establishing a Texas Coordinator of Cybersecurity within the Office of the Governor** to provide a strategic direction to bring government and business leaders together as partners in securing the state's infrastructures and developing a strategy and plan to promote the cybersecurity industry within the state.
- 2. Establishing the Business Executives for Texas Security (BETS) partnership** to bring public- and private-sector leaders and cybersecurity practitioners together to form a framework for knowledge sharing and collaboration, making non-proprietary and industry-recognized best practices and solutions readily available for the collective improvement of cybersecurity across the state.
- 3. Establishing a "Cyber Star" program** to foster improvement of cyber resiliency in both private and public infrastructures across the state and to increase public trust by establishing a baseline for responsible cyber operations.
- 4. Adopting the Community Cyber Security Maturity Model as a statewide guide** for developing a viable and sustainable cybersecurity program and fostering a culture of cybersecurity throughout the state.
- 5. Increasing the number of cybersecurity practitioners in Texas** to provide the expertise needed to grow cybersecurity investment and to protect the cyber assets of the state.

- 6. Providing a consistent voice for industry** regarding cybersecurity policies in order to facilitate communication between the state and industry.
- 7. Continuing investment in higher education cybersecurity programs** in order to attract students to the cybersecurity field, spur research and development, and encourage institutions of higher education to become leaders in cybersecurity within their own communities.
- 8. Promoting collaboration, innovation, and entrepreneurship in cybersecurity** to facilitate the commercialization of university research and development and encourage the development of new businesses with innovative products and services in cybersecurity.
- 9. Developing a comprehensive cybersecurity education pipeline through the BETS partnership** to introduce cybersecurity initiatives from K–PhD.
- 10. Reviewing and sharpening the leadership role of the Texas Department of Information Resources (DIR)** in establishing a sustainable Cybersecurity Awareness Program for all Texans.

Introduction

Texas Economy and Critical Technology Infrastructures at Risk

Cybersecurity threats continue to evolve and are outpacing Texas organizations' ability to protect the state's cyber environment, compromising the physical safety, financial security, and privacy of Texas citizens. Public, non-profit, and commercial entities within the state are challenged to collaboratively identify and mitigate large-scale cyber events by national and international entities with intent and ability to cause critical outages, steal private information, or harm Texas government and business in other ways.

In response to the rapidly expanding Texas and national cyber threat landscape, the 82nd Texas Legislature took steps in 2011 to leverage public/private partnerships to examine the infrastructure of the state's cybersecurity operations. These operations include the administrative and technical measures taken to protect business against unauthorized access or attack, including preventing criminal or unauthorized use of electronic customer data. The effort is intended to produce strategies to accelerate the growth of cybersecurity as an industry within Texas. This includes both cybersecurity businesses that create and market security products and services, as well as those businesses with significant cybersecurity operations requirements. The goal is to encourage all industry members to call Texas "home."

The Texas Cyber Environment Today

The U.S. cyber environment is clearly at risk. From October 2011 through February 2012, more than 50,000 cyber-attacks on private and government networks were reported to the U.S. Department of Homeland Security, including 86 attacks against "critical infrastructure networks." These attacks, regardless of originating country, likely represent a small fraction of cyber-attacks carried out in the United States. It is important to note that cyber-attacks are not confined to the realm of cyberspace. A cyber-attack can also inhibit, intrude upon, or damage physical property such as machines, motors, and physical processes controlled by computers. Today, underlying control systems and technologies are converging due to the acceptance of Internet Protocol (IP) as the *de facto* method of linking these systems. Thus, the cyber environment includes a symbiotic relationship with virtually all public and private economic clusters because of the computers, software, telecommunications, and embedded control systems at the heart of critical infrastructure.

Texas organizations rely on the state's cyber environment to deliver many commercial, government, and education products and services to Texas' more than 26 million citizens. The Texas environment includes public organizations such as state agencies, higher education institutions, local governments, K-12 education, and emergency management districts, as well as private entities. This environment also encompasses for-profit and not-for-profit corporations, including faith-based organizations, 50+ U.S. Fortune 500 companies headquartered in Texas, and many U.S. and global firms with significant business operations in the state. Texas business must ensure it effectively and continuously protects the state's cyber environment in order to support the Texas economy.

The Texas cyber environment, including critical infrastructures such as water, energy, healthcare, banking, and transportation, is shared and governed by a myriad of Texas public and private organizations with differing organizational missions and regulatory requirements for privacy and security. Each organization is required to establish and maintain appropriate cybersecurity operations, processes, and technologies and hire trained, professional cybersecurity staff to protect their operations and the information entrusted to them by Texas citizens.

Looking Back: SIPAC Assessment of Texas Critical Infrastructure

The state's critical infrastructures were the subject of the 2001 State Infrastructure Protection Advisory Committee (SIPAC) assessment commissioned by the Texas Attorney General. SIPAC was charged to review Texas' critical infrastructures and make recommendations for protecting this portion of the Texas cyber environment.

The SIPAC report, released in 2002, focused on state agency, higher education, and emergency management. It proposed creating many strategic, tactical, and operational Texas homeland security and technology infrastructure protection capabilities for state critical infrastructures. The enhancements implemented as a result of SIPAC's recommendations included creating the Texas Department of Homeland Security. Additionally, the Texas Department of Information Resources (DIR) created plans, strategies, policies and related operations and services capabilities related to protection of critical technology infrastructures. Many Texas critical infrastructures are also now subject to compliance with federal government and industry security requirements that have influenced public and private organizations to invest in improving their cyber operations capabilities.

While SIPAC spurred statewide efforts, and further federal regulation has helped advance many of SIPAC's critical infrastructure goals, these efforts have neither extended to non-critical infrastructure portions of the state's cyber environment nor led to the coordination of protection activities between Texas public and private organizations.

Senate Bill 988 Charge and Council Analysis and Assessment

Fiscal year 2011 legislation, through Senate Bill (SB) 988, charged DIR with appointing nine members from across government, academia, and industry to form the Texas Cybersecurity, Education, and Economic Development Council. The Council is responsible for conducting an interim study and providing recommendations to DIR's Executive Director regarding ways to 1) improve the infrastructure of the state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cybersecurity as an industry in the state. The Council is required to submit its findings by December 1, 2012, to the

- DIR Executive Director
- Governor
- Lieutenant Governor
- Speaker of the House of Representatives
- Higher Education Committees of the Senate and House of Representatives

- Senate Committee on Economic Development
- House Technology Committee
- House Economic and Small Business Development Committee

The Council focused on analyzing the cybersecurity economic development context, cybersecurity education capabilities, and cyber operations for the state's cyber infrastructure environment, both public and private. In performing the analysis, the Council conducted an online survey of government and business organizations; analyzed DIR's database of state agency information resources survey responses; held face-to-face and "virtual" meetings with Texas and federal cybersecurity workforce, education, and training experts; and met with Texas and national cybersecurity infrastructure experts on emerging federal and private enterprise cybersecurity infrastructure trends. The Council performed a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of statewide cybersecurity infrastructure, industry, and education capabilities.

The results of this analysis are below.

Strengths

- DIR has established a strong information security program for state agencies and is capable of taking on a greater leadership role in cybersecurity.
- Texas has a great track record in attracting new industry and providing a good environment for business operations.
- Texas has many current private-sector champions to support growth of the cybersecurity industry within Texas.
- Good models exist for successful metro area participation in cybersecurity programs and innovation centers ("Pockets of Excellence").
- Texas has 12 National Security Agency (NSA)/ Department of Homeland Security (DHS) Centers of Academic Excellence in Information Assurance Education and/or Research tied to higher education.
- Texas Administrative Code 202 provides a good framework for securing cyber infrastructure.

Weaknesses

- Both private- and public-sector organizations have developed internal cybersecurity activities that are often sub-optimized. Best practices are not shared.
- There is no centralized database for contacts and communications processes for organizations in Texas.
- Resources have not been quantified for cybersecurity activities.
- There is not an established forum for industry to participate with state government for enhancing cybersecurity in Texas.
- There is a general lack of awareness regarding securing the cyber infrastructure.
- There is an insufficient number of qualified, trained cybersecurity personnel to meet industry demand.

Opportunities

- There is an alignment of thought around cybersecurity by Texas industry and state government leaders.
- Best practices in cybersecurity activities can be shared and replicated (scalable).
- Cybersecurity awareness has increased at the federal level. Federal reports and other resources regarding cybersecurity, especially information, are becoming available.
- Cybersecurity training resources may be available from certain state agencies and higher education institutions. These existing resources can be harnessed to create a centralized repository of cybersecurity knowledge and skills in Texas.
- Media has begun covering major cybersecurity incidents.

Threats

- Sophistication of attackers is increasing (e.g., nation states, organized crime, hacktivists).
- The number and severity of cybersecurity exploits have increased.
- The nature of cybersecurity exploits has become more threatening (i.e., the scope of impact spans national security compromises, economic loss, terrorism, and the standard factors of nuisance and personal loss).
- Rapid advancements in technology (e.g., mobile computing, social networks, and cloud computing), coupled with a large population of computer users under-educated in cybersecurity awareness creates an environment ripe for major losses and damages caused by cybersecurity exploits.
- As critical infrastructure resources (e.g., energy and water) become increasingly dependent on computing networks for operations and maintenance, they also become potential targets for cybersecurity exploits. These critical infrastructure resources are, however, prerequisites for industry growth in Texas.

Council Call for Action

Texas must establish a statewide focus for the Texas cyber environment, one that extends beyond critical infrastructure networks to include Texas business and public leaders in collaborative efforts to identify and mitigate risks and threats to Texas citizens and to spur innovation in the cyber environment. The Council recommends Texas executive and legislative branches consider establishing a framework for designating oversight of cybersecurity coordination and for a sustainable private/public-sector partnership working jointly to improve the state's cybersecurity posture and to protect and enhance its economy. Texas must enable this framework for action by defining specific statewide authority, influencing adoption across non-government industry, creating special public-private partnerships, designating funding authority or sources for sustainability and growth, and considering impact of emerging cyber threats and cyber regulation challenges. This will allow Texas to continuously enhance statewide cybersecurity infrastructure and education capabilities and advance statewide cybersecurity economic development through business expansion, recruiting, and research and development commercialization efforts. These structures and processes are needed to ensure that Texas effectively and continuously designs, implements, and upgrades cybersecurity operations, hires and retains trained and capable cybersecurity workers

to manage the state's cyber risk, and creates statewide cybersecurity industry and cybersecurity industry opportunities.

Findings and Recommendations

To fulfill its charter, the Council explored findings and recommendations in three key areas:

- Texas' cybersecurity **infrastructure** was analyzed in an effort to develop recommendations that could lead to improving both the state's cybersecurity infrastructure and its ability to coordinate cybersecurity efforts among non-governmental elements within the state.
- **Industry**, a vital part of the cybersecurity environment, was examined from two standpoints—first from the perspective of how the security of cyber assets in the state's industries could be improved and, second, how more industry could be attracted to the state to spur greater economic development.
- The Council examined **education** from the perspective of both formal degree and certification programs as well as general awareness of cybersecurity issues within the state.

Advancing Cyber Secure Infrastructure in Texas

Findings

The cybersecurity strengths and opportunities that already exist within Texas demonstrate significant potential for advancing a more secure cyber infrastructure across the state. However, the weaknesses and threats identified during the Council's deliberations resulted in three significant findings that drove development of recommendations for infrastructure improvement.

There is no single lead office for cybersecurity coordination of policy and response in Texas.

Although the Council deems DIR's Information Security Program for state agencies a major strength, and although Texas Government Code does, in fact, name DIR's Executive Director as the State Chief Information Officer, the powers and duties of that position outlined in the code, as well as those of DIR itself, are limited mostly to procurement and security oversight within state agencies and do little to generate and coordinate the partnerships between public and private entities that are necessary to the collective cybersecurity of Texas (*Texas Government Code, Sections 2054.0285, 2054.052 regarding duties and powers of the Executive Director and the Department of Information Resources*).

Lack of a coordinated cybersecurity effort across the state allows malicious cyber activities to outpace the development of a secure infrastructure to effectively counter those activities. To gather information about the current state of the cybersecurity infrastructure in Texas, the Council surveyed organizations throughout Texas. This effort uncovered a significant impediment to obtaining valid survey results across multiple sectors, namely the lack of an established statewide comprehensive contact list of cybersecurity leads for all levels of state, county, and municipal government along with major Internet service providers, other telecommunications companies, military installations, and critical infrastructure. This is a critical state deficiency affecting both proactive and reactive cybersecurity efforts, as well as potentially affecting other state operations.

The Council found several examples of innovation and cyber excellence in and around major metropolitan areas and military installations; however, these efforts are mostly localized rather than programs to expand to regional or statewide models. The commitment of cities such as San Antonio, whose elected leadership, Chamber of Commerce, businesses, military community, universities and colleges, and independent school districts have joined in a focused collective effort to increase cybersecurity education and awareness by leveraging opportunities in the areas of people, process, and technology have resulted in nationally recognized cybersecurity success. These models should be considered across the state. There are other examples of innovation and achievement in cybersecurity throughout Texas. For example, Figure 1 shows the list of NSA/DHS Centers of Academic Excellence in Information Assurance found in Texas.

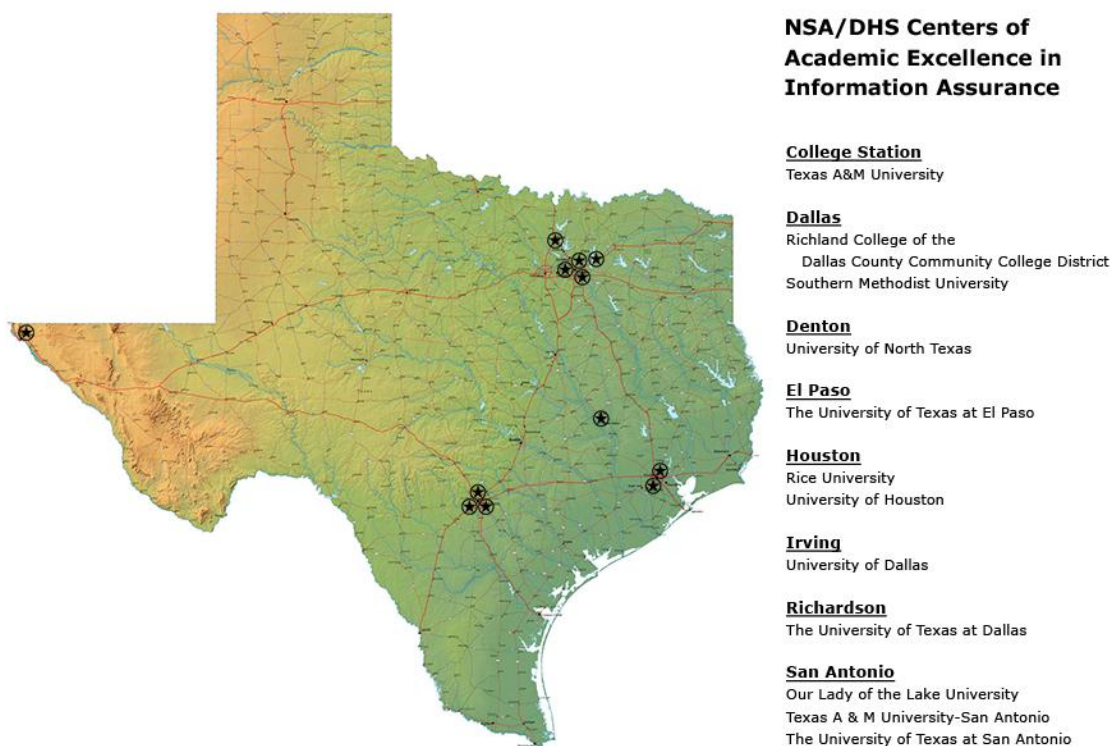


Figure 1. NSA/DHS Centers of Academic Excellence for Information Assurance in the State of Texas

Although these centers for advancement exist in Texas, a significant gap remains between the levels of resourcing that private industry expends for cybersecurity and the levels of resourcing available to state and local governments, school districts, and other non-profit entities. In most instances, the question is not whether to establish a cybersecurity program, but rather where to start. The absence of a generally accepted baseline against which less densely populated and rural communities, small businesses, non-profit organizations, utility districts, and school districts can use to measure progress toward cyber maturity leaves these organizations, and by extension the citizens and customers they serve, persistently vulnerable.

Recommendations

Whether large or small, whether mature or just getting started, Texas' cybersecurity infrastructure is an interconnected chain of systems that is only as strong as the weakest link. The Council proposes five strategic actions for advancing Texas' cyber secure critical infrastructure:

- Establish a Texas Coordinator of Cybersecurity within the Office of the Governor.
- Establish the Business Executives for Texas Security (BETS) Partnership.
- Establish a "Cyber Star" program to foster improvement of cyber resiliency in both private and public infrastructure in the state as well as increasing public trust.
- Adopt the Community Cyber Security Maturity Model (CCSMM) as a statewide guide for developing processes leading to a state of cyber maturity.
- Expand and strengthen DIR's duties and powers.

Establish a Texas Coordinator of Cybersecurity within the Office of the Governor.

Improving cybersecurity for a state the size and complexity of Texas requires a heightened synergy of effort as well as different leadership expectations to address the question of "who's in charge" when it comes to cybersecurity.

While DIR has performed well in this role and should continue to perform this function for the diverse agencies and departments of state government, Texas requires a charismatic and empowered leader who has the support of the Office of the Governor and possesses the authority and the initiative to bring influential government and business leaders together as partners in the interest of a statewide cybersecurity agenda. Cybersecurity is pervasive and impacts virtually all industries and government sectors while at the same time representing an overlooked industry cluster with a unique opportunity for wealth creation through concerted research, development, and commercialization efforts.

This recommendation does not come without some historic challenges. Creating new functional organizational coordinators or "czars" often fails because they are given great responsibilities but few authorities to necessitate collaboration across diverse agencies and departments as well as the private sector and higher education.

Improved collaboration between public and private sectors on advancing the collective cybersecurity of the state requires support of executive leadership. To best ensure success, the Council recommends the active participation of the Office of the Governor to encourage proactive engagement from other senior leaders of public and private sectors. Economic development initiatives will also benefit from executive leadership in convening the marketplace and exploring opportunities in partnership with the Texas Enterprise Fund, the Texas Emerging Technology Fund, and emerging insurance and risk management markets. Figure 2 depicts the central role the Texas Coordinator of Cybersecurity would play in synchronizing cybersecurity efforts in the state.

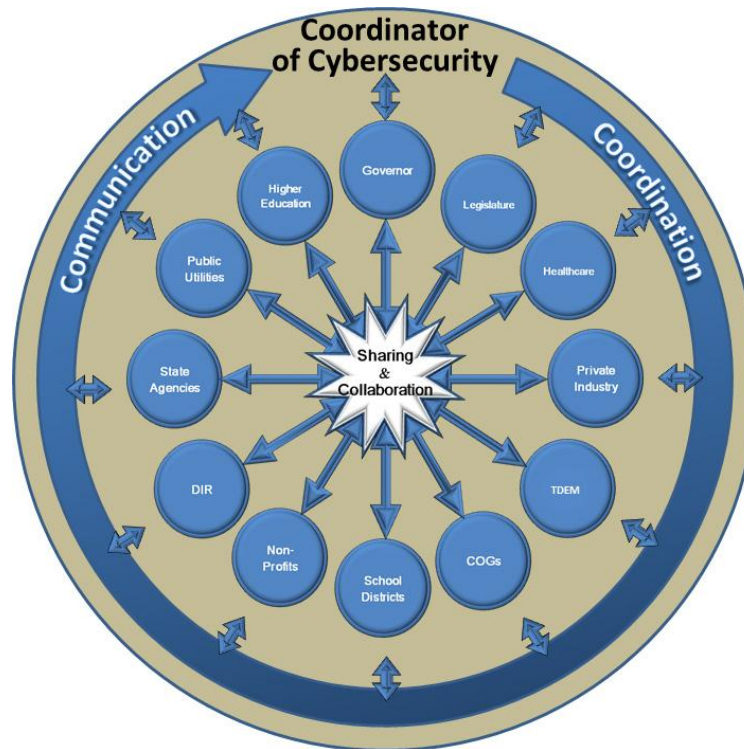


Figure 2. Coordination of Cybersecurity among Organizations

Establish the Business Executives for Texas Security (BETS) Partnership.

The challenges confronting the state's cybersecurity infrastructure are multifaceted, interrelated, and numerous. They require the collective knowledge and effort of both public and private sector entities to expedite infrastructure improvement and move the state beyond reacting to threats to an environment of more proactive prevention and protection.

For this reason, the Council recommends that the Office of the Governor, through the state Texas Coordinator of Cybersecurity, charter and facilitate a Business Executives for Texas Security (BETS) organization that unites public and private sector leaders and cybersecurity practitioners in a partnership that enables the creation of an enduring framework for knowledge sharing and collaboration, making non-proprietary and industry-recognized best practices and joint solutions more readily available for the collective improvement of cybersecurity across the state.

This group, in partnership with the state and higher education, can establish a coherent, continuing framework that will:

- Define what cybersecurity means to Texas in a succinct uniform statement of purpose.
- Provide objective feedback to the executive branch regarding proposed cybersecurity policy.
- Establish generally accepted and fundamental norms for all phases and functions of cybersecurity in Texas.
- Develop joint solutions to security problems in Texas.

- Promote government-industry partnerships and encourage participation in organizations such as the FBI-sponsored InfraGard program and other professional organizations that can help to foster government-industry relationships.
- Encourage pooling of cyber talent from industry and government with academia to facilitate collaboration between individuals and organizations with similar research interests.

Appendix D contains additional details regarding background as well as proposals for both organization and structure of the BETS Partnership.

This recommendation sets conditions for significant improvement in networking and collaboration between government and business leaders as well as cybersecurity professionals across the state toward the end of seizing the initiative and transitioning the state's cybersecurity to a more proactive posture.

Establish a “Cyber Star” program to foster improvement of cyber resiliency in both private and public infrastructure in the state as well as increasing public trust.

The program is modeled after the U.S. Department of Energy's “Energy Star” program, but would focus on the cybersecurity practices of agencies and companies rather than the energy efficiency of a product.

Participation in such a program would be voluntary and aimed at validating that the applicant:

- Maintains a program to keep its workforce educated and aware of the importance of cybersecurity.
- Uses generally accepted cybersecurity best practices and processes.
- Conforms with standards relative to cybersecurity (e.g., SANS Twenty Critical Security Controls for Effective Cyber Defense).
- Performs regular internal and external assessments of their cybersecurity program.
- Demonstrates that they use appropriate and secure technology in business processes and practices.

Figure 3 depicts how the five points of the Cyber Star, together with participation and input from public and private sector stakeholders, supports a well-rounded cybersecurity program. Appendix E discusses the general concept, key objective, and suggestions for establishing this program.

The Council believes that such a program developed and embraced by BETS with a distinct certification logo that can be displayed on an agency's or company's public website will allow potential customers to easily identify organizations with whom doing business or e-business is safe from a cybersecurity standpoint.

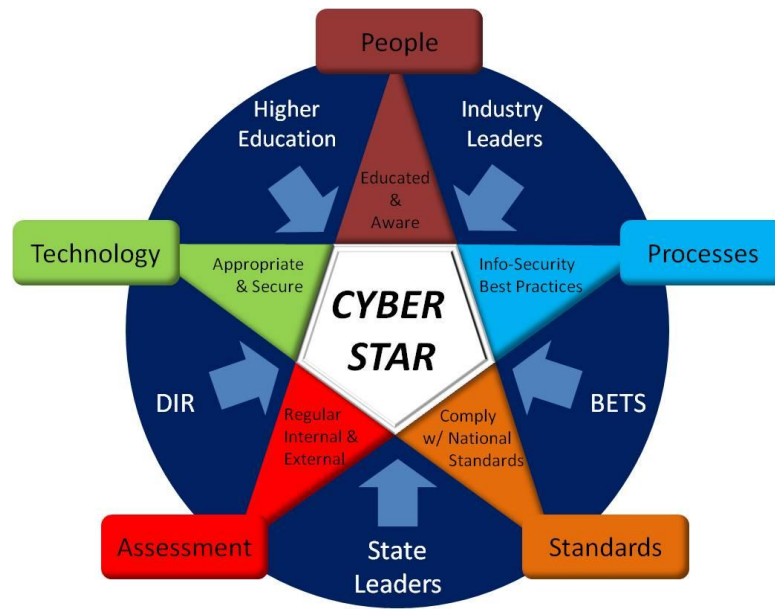


Figure 3. The Cyber Star Program

Adopt the Community Cyber Security Maturity Model (CCSMM) as a statewide guide for developing processes leading to a state of cyber maturity.

Rural communities, municipalities, and counties as well as small businesses and non-profit organizations traditionally face a tremendous task in prioritizing available resources to maintain the availability of services their constituents, customers, and clients rely on, and that must occur before consideration is given to any kind of cybersecurity program. Even well-resourced communities, governments, and organizations are often challenged in knowing where to start and what to place emphasis on when developing a comprehensive program for protecting not only the information systems and networks that connect them but also the critical infrastructures that enable these systems to function.

Developing and using maturity models is a recognized method for providing a uniform guide for establishing processes that lead to a state of maturity in an area for which the model was built. The CCSMM evolved from the need to determine the cyber preparedness of a community and to identify a prioritized plan to improve the level of preparedness. The CCSMM guides community leadership through an assessment that results in categorizing where a community fits in one of five levels of maturity:

- **Level 1 – Security Aware:** Make individuals and organizations aware of threats, problems, and issues related to cybersecurity.
- **Level 2 – Process Development:** Establish and improve on the processes required to effectively address cybersecurity issues.
- **Level 3 – Information Enabled:** Ensure that all organizations within the community are aware of the issues related to cybersecurity and have established the processes and mechanisms necessary to identify security-related events.

- **Level 4 – Tactics Developed:** Ensure that programs are designed to develop more efficient and more proactive local and strategic methods to detect and respond to attacks.
- **Level 5 – Full Security Operational Capability:** Illustrate how the top level of the model represents that the necessary processes and tools are in set in place to enable any organization to consider itself fully capable of detecting and addressing any type of cyber threat.

After determining at which level the community currently resides, the CCSMM helps leaders determine what must be accomplished in order to improve the current state of cybersecurity and better prepare to respond to cyber attacks. Appendix F contains more detailed information regarding the needs that drove the development of the Community Cyber Security Maturity Model, as well as some of the early successes resulting from its use.

Expand and strengthen DIR's Duties and Powers.

DIR's successes in recent years to develop and implement cybersecurity for state agencies must be capitalized upon and its role further developed to enable the continued growth of a comprehensive cybersecurity plan for the state's public infrastructure.

To the extent that Texas legislation currently addresses the topic of cybersecurity at all, the focus is primarily on one of reaction to a cyber crime and potential punishments (Title 7 Texas Penal Code, Chapter 33 regarding Computer Crimes) rather than any focus on prevention or protection against malicious cyber activities.

Despite best efforts, cyber crime and incidents will continue, and the need to respond remains. But just as important to the overall cybersecurity effort is identifying vulnerabilities and taking proactive measures before incidents occur. To that end, Texas Government Code sections regarding DIR's duties and powers should be reviewed and updated, and resources identified, in order to enhance DIR's efforts to lead implementation of state infrastructure improvement activities. These activities would be executed in conjunction with the Texas Coordinator of Cybersecurity and would focus on improving the state's prevention of and defense against cybersecurity incidents.

Infrastructure Summary

Advancing a cyber secure infrastructure is the foundational element for moving toward a more secure and prosperous Texas. The willingness of private industry in Texas to participate in and support focused efforts to improve cybersecurity in major metropolitan areas, as demonstrated in San Antonio, significantly raises the potential for meaningful exchange of best practices and information sharing between public and private sectors. The establishment of a Texas Coordinator of Cybersecurity in the Office of the Governor is key to seizing this opportunity and capitalizing on it for the long-term benefit of the state.

Developing the Cybersecurity Industry in the State

Findings

The Council was charged with examining specific actions to accelerate the growth of cybersecurity as an industry in the state. Regardless of the industry, the foundation for all business growth in the

state remains the same. There is no substitute for a reasonable and reliable regulatory climate, low taxes, a resilient and modern infrastructure, and a skilled workforce. Those core attributes have remained strong in Texas and are the key reasons for the state's economic strength. They are as applicable to the cybersecurity industry as they are to any other industry within the state. Since the cybersecurity industry as a whole is vital to both the state and national economy, the Council has identified five findings within industry and produced recommendations for possible solutions to those concerns:

- To grow cybersecurity investment in Texas, the industry requires access to more trained cybersecurity professionals, financial capital, and cybersecurity innovation.
- Texas must invest in cybersecurity education programs across the K–12, community college, and university levels in order to obtain the number of trained cybersecurity professionals it needs across the employment continuum.
- Texas lacks a statewide context and strategy for advancing cybersecurity industry economic development.
- There is no consistent voice for industry regarding cybersecurity policies and recommendations in the state.
- There is not enough cybersecurity collaboration, innovation, and entrepreneurship within the state.

To grow cybersecurity investment in Texas, the industry will need access to more trained cybersecurity professionals, financial capital, and cybersecurity innovation.

The Council conducted a formal survey to determine the current state of Texas' cybersecurity programs. Appendix G contains a discussion of the survey. In addition, the Council informally surveyed numerous for-profit companies, both large and small, as well as federal government agencies to include the U.S. Department of Defense (DoD). **The lack of a qualified workforce was universally cited as the single largest challenge to the productivity and growth of this industry.** In addition, individuals surveyed at the DoD and major defense contractors cited serious concerns over their difficulty in finding qualified personnel who were U.S. citizens capable of receiving the required security clearance for their work. This led to the next finding.

Texas needs to invest in cybersecurity education programs across the K–12, community college, and university levels in order to obtain the number of trained cybersecurity professionals it needs across the employment continuum.

IT professional shortages exist at three critical educational levels: certification (sub-two year degree), associate's degree (sub-baccalaureate degree), and bachelor's and post-graduate degrees. To be effective, employers, including the military and homeland security professionals, should determine the skills, knowledge and competency requirements. To address these needs, national cybersecurity skill standards were developed through a National Science Foundation Advanced Technological Education (ATE) center grant to Bellevue College in Washington State in 2003. These skill standards are aimed at the entry-level employee and are most commonly used as the basis for AAS degrees. They were recognized by the Texas Skill Standards Board and are currently available to community and technical colleges to inform curriculum alignment with employer skill needs.

However, many years have passed since those standards were developed, and the technology landscape has changed significantly during that time. As a starting point, they could provide the foundation to create new standards to meet current employer needs and provide the starting point to address curriculum development at all levels. More recently, in 2011, the National Institute of Standards and Technology (NIST) initiated the National Initiative for Cybersecurity Education (NICE) and recently published the National Cybersecurity Workforce Framework. The framework is another possible starting point to form the basis for updating Texas' cybersecurity workforce programs for high school career and technical education, community college workforce programs, and even professional education in universities.

The Council noted the work of The University of Texas at San Antonio (UTSA) and the Alamo Community College District's Information Technology and Security Academy (ITSA), as well as the support from large corporations such as USAA and Rackspace, which is well known throughout the rest of the nation and is often cited as an example of an effective focus on the issues related to cybersecurity. That reputation was earned through significant support of regional, state, and national programs developed at institutions of higher education in San Antonio. Those centers of excellence, such as The Institute for Cyber Security at UTSA, which was originally formed with funding from the Texas Emerging Technology Fund, have used state funds to leverage significant federal and other non-state funds back into UTSA and the state. Outside of San Antonio, The University of Texas at Austin's Center for Identity is another example of Texas programs leveraging non-state dollars to grow and develop their cybersecurity programs.

Texas lacks a statewide context and strategy for advancing cybersecurity industry economic development.

For a cybersecurity business to thrive in Texas, it will need access to several other key ingredients: capital, markets, technology transfer opportunities, a culture for innovation, and a healthy business climate, among others. Texas certainly has much to offer in these areas, including world-class university systems, key federal cybersecurity assets, a business-friendly climate, and a mature venture capital ecosystem. When the Governor convened the Industry Cluster Initiative in 2005, the IT cluster group discovered that federal research and development (R&D) investment in Texas over the ten-year period, 1993–2003, represents a capture of only one half of one percent—\$204 million of \$41 billion invested. This cyber initiative is in part about spurring innovation through R&D and capturing a greater percentage of emerging network and information technology R&D, companies and start-ups within the state. Assembling these elements into a mixture optimal for a thriving cybersecurity business climate is critical and requires considerable thought. In short, a comprehensive strategy describing a clear plan on how to accelerate growth of the cybersecurity industry in Texas does not presently exist, and the creation of such a strategy is needed at this time.

There is no consistent voice for industry regarding cybersecurity policies and recommendations in Texas.

Texas recognizes that cybersecurity influences all forms of business throughout the state, from small business to Fortune 500 companies, as well as multiple state and federal agencies inside of Texas. As

such, a formal, consistent voice for industry regarding cybersecurity policies and recommendations is needed.

There is not enough cybersecurity collaboration, innovation, and entrepreneurship within the state.

Texas could benefit from more opportunities for proactive cybersecurity collaboration and entrepreneurship. San Antonio is home to one example of this general sort of activity in the form of a unique collaborative environment known as “Geekdom.” The primary goal of the program is to foster ideas and entrepreneurship in technology and to provide mentorship and assistance in a collaborative setting. Such efforts have a proven track record of “connecting the innovation dots” and increasing the entrepreneurship activity of a community.

Recommendations

Based on its understanding of the cybersecurity industry within Texas and what is needed to increase the cybersecurity industry presence within the state, the Council explored the following recommendations:

- Develop a comprehensive strategy and plan that describes how Texas will create a vibrant and robust cybersecurity industry and economy.
- Increase the number of cybersecurity professionals in the state.
- Provide a consistent voice for industry regarding cybersecurity policies.
- Continue investing in higher education cybersecurity programs.
- Promote collaboration, innovation, and entrepreneurship in cybersecurity.

Develop a comprehensive strategy and plan that describes how Texas will create a vibrant and robust cybersecurity industry and economy in the state.

The state must have an understanding of what is needed to create an environment that is enticing to the cybersecurity industry. The goal is to use this understanding to establish a strategy and direction which will help to create this environment to promote cybersecurity industry within the state. Consideration must be given to the way Texas cybersecurity businesses will gain access to people, capital, markets, technology transfer opportunities, a culture of innovation and entrepreneurship, and other factors that will lead to the growth of the industry. Discussions with leaders from other states that have made cybersecurity a statewide priority, such as Maryland, will be valuable in incorporating best practices.

Finally, the industry and economic growth strategy that must be created must ensure proper coordination with critical infrastructure considerations so that the right balance of economic growth and infrastructure development is met. During the 1980s, SEMATECH was formed in Austin to support the national security needs of the nation by acting as a hub for shared research and development in the non-competitive domain of semiconductor manufacturing. Today, a similar opportunity exists to form an organization focused on computer, software, network, and human systems related to cybersecurity.

Increase the number of cybersecurity practitioners in Texas.

Through the information gathering by Council, it was revealed that Texas lacks the number of cybersecurity professionals it needs to both secure its own assets as well as to encourage additional industry to locate within the state. Texas must increase its number of cybersecurity professionals for both the cybersecurity industry and industry in general.

Increasing the number of cybersecurity practitioners is important, but it can't be done without developing an understanding of the skills needed by our business community. There are many aspects to cybersecurity often requiring unique skill sets. In cooperation with our industry partners, the state must determine what specific cybersecurity skills are needed and establish a method to address this need. The BETS organization should work to identify skills, knowledge, and competencies required for entry-level positions and then work with the Texas Higher Education Coordinating Board (THECB) and the Texas Skills Standards Board to revise and update standards for degrees based on the competencies identified.

Many factors affect the number of individuals who desire to pursue an education in cybersecurity-related disciplines. Increasing the number of cybersecurity practitioners requires more than just addressing the curriculum issues. Addressing issues directly impacting students must also be considered, including:

- Instituting post-secondary loan forgiveness for critical cybersecurity degrees.
- Initiating an aggressive campaign to inform students, parents, and educators of the supply and demand gap, along with real time data on wages to incent behavioral change at the educational front end.
- Identifying barriers at institutions of higher education to eliminate attrition rates within IT degree plan.
- Encouraging four-year institutions of higher education to work closely with two-year institutions to establish articulation agreements enabling students to advance their cybersecurity educational opportunities.

Provide a consistent voice for industry regarding cybersecurity policies.

Texas must address the need for a representative and consistent voice for industry regarding cybersecurity policies and recommendations. This entity can facilitate communication in both directions—from the state to industry and from industry to the state. The industry and economic growth strategy that must be created needs to ensure proper coordination with critical infrastructure considerations so that the right balance of economic growth and infrastructure development is met. This entity can go a long way toward establishing a single entity within the state to provide a consistent voice on cybersecurity issues for industry. This entity, whether BETS specifically or another advisory group formed in response to this recommendation, should:

- Provide policy development assistance to DIR and the Texas State Legislature.
- Be appointed by the Governor and have legislative authority to form additional committees, invite members, and form additional support groups.
- Meet at least annually to provide recommendations to DIR's Executive Director or at the request of the Governor or the Legislature.
- Receive support funding from the state or through the Texas Economic Development Corporation (Texas One).

Continue investing in higher education cybersecurity programs.

An earlier recommendation addressed the need to develop curricula as well as programs to attract students to the cybersecurity field. The state must also recognize the importance of higher education to the cybersecurity efforts and encourage continued support of programs at this level. This can be accomplished through a number of initiatives including:

- Recognizing the benefit of higher education infrastructure development in cybersecurity by continuing to fund efforts at established centers of excellence, as well as developing new programs in cooperation with existing centers throughout the state.
- Funding for the centers of excellence and new programs through the regular biannual legislative progress or through existing state programs such as the Texas Emerging Technology program.
- Facilitating private industry cooperation through incentives in the funding of additional centers of excellence and requiring centers within the state to foster collaboration opportunities.
- Encouraging institutions of higher education to become Community Centers of Excellence in Cybersecurity to help their own communities establish and maintain viable and sustainable cybersecurity programs.

Promote collaboration, innovation, and entrepreneurship in cybersecurity.

Texas should highlight the benefits of collaborative efforts between education and industry and encourage the development of new businesses with innovative ideas in cybersecurity. Initiatives in this regard would include:

- Texas encouraging the continued development of collaborative entrepreneurship program, such as "Geekdom," throughout the state.
- Texas Institutions of Higher Education working directly with industry and non-profit organizations to develop collaborative entrepreneurship programs in their areas.
- Texas providing additional funding through university participation or through specific legislative appropriation.
- Utilizing existing organizations such as the alumni networks found in the UT and Texas A&M systems to encourage entrepreneurs and establish partnerships.

Industry Summary

As illustrated in the recommendations in this section, economic development cannot be accomplished without establishing a culture of cybersecurity within Texas. Cybersecurity does not exist solely in any one sector but is found across the spectrum of government, academia, and industry. The Council's chief findings and recommendations in this area highlight the need for better

coordination between the state and industry and reiterate the importance of the development of an entity such as BETS while also identifying the need for more cybersecurity practitioners. The next section speaks to the creation of the overarching need for the establishment of a cybersecurity culture within the state.

Creating an Enduring Cybersecurity Culture

Findings

There were two key Council findings regarding cybersecurity education in Texas. First, the education and professional training institutions in Texas are not producing enough qualified cybersecurity professionals to meet the needs of employers in Texas. A poll conducted by this Council of key business leaders in Texas indicates a shortage of a qualified cybersecurity workforce in Texas. A similar finding at the national level is reflected in a November 2010 federal report from the Center for Strategic & International Studies (CSIS), titled “A Human Capital Crisis in Cybersecurity.” Secondly, the Council found that Texas lacks a coordinated and developed cybersecurity awareness program for Texans.

Recommendations

Both findings can be addressed by creating an enhanced and coordinated cybersecurity education program in Texas. The term “education,” as used in this report, includes education as delivered through institutions of learning, professional training, and awareness training. The audience for cybersecurity education can be generally categorized as “cybersecurity practitioners” and “all other Texans.” The term “practitioners” includes both cybersecurity professionals and information technology professionals. Cybersecurity education for practitioners must lead to positive job placements in the current and future marketplace.

Accordingly, the education curricula would be different for these two groups. The types of education programs that would be focused for cybersecurity practitioners should include the following:

- Masters, PhD, and post-doctoral formalized educational programs that include both education and research components.
- Four-year degrees focusing on cybersecurity areas—generally in computer science, information systems, computer engineering, cybersecurity, information assurance, or related fields.
- Two-year associate degrees, diplomas, or certificates in information systems, cybersecurity, information assurance, or related fields.
- Industry and educational institution-delivered cybersecurity-related professional training that prepares students for cybersecurity-industry recognized certifications.

For all other Texans, a general cybersecurity awareness curriculum should be developed. Cybersecurity awareness programs should be ongoing, and the curriculum contents should be current, relevant, succinct, and easily available.

A number of good strategies have been outlined at a national level to address the cybersecurity workforce development and to improve other aspects of cybersecurity education. This report does not plan to duplicate those strategies but instead provides some actionable recommendations.

However, there may be opportunities to leverage some of the national strategies as part of implementing certain recommendations made in this report.

BETS should include a senior representative from THECB and from the Texas Education Agency (TEA). Subsequent working groups could leverage expertise from the education community and other agencies as appropriate.

As a first step, BETS should set in motion activities to create the Texas Cybersecurity Education Pipeline (see Figure 4 below). A major activity toward building a successful Cybersecurity Education Pipeline is to enhance and coordinate existing science, technology, engineering, and mathematics (STEM) programs as well as computer science and IT elective programs in schools as these programs form the general basic pool from which cybersecurity studies, and subsequently cybersecurity graduates, can be developed.

BETS, working with appropriate partners, should also explore options to introduce new cybersecurity education curriculum in junior high and high schools, actively promote dual credit programs in high schools in the cybersecurity field (similar to the Information Technology and Security Academy, one of the Alamo Academies in San Antonio), develop robust regional Programs of Study (also known as “career pathways”) with local independent school districts, community colleges, and universities, encourage professional mentorship of students, and establish community college and higher education collaborations for those seeking advanced cybersecurity degrees. Formalized cybersecurity education curricula should also produce graduates who are prepared to earn industry-recognized professional IT certifications such as A+, Network +, Security +, CCNA, CISSP, CISM, GIAC, etc.

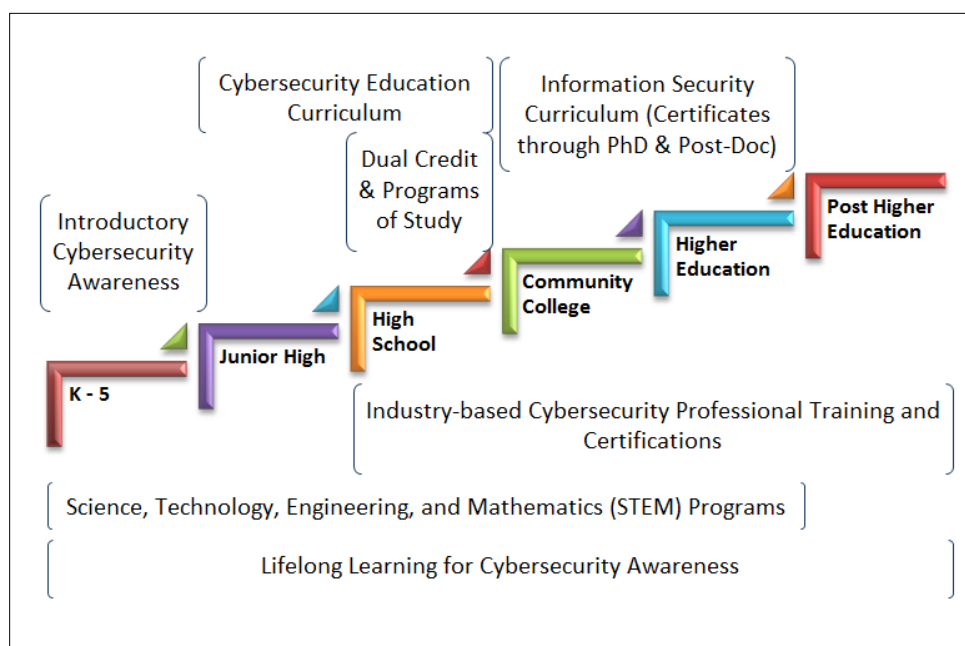


Figure 4. Proposed Texas Cybersecurity Education Pipeline

In addition to exploring new and innovative ideas and partnerships to promote the Cybersecurity Education Pipeline, BETS can also help to facilitate the coordination and growth of existing innovative programs such as the CyberPatriot high school cyber defense competition, the National Collegiate Cyber Defense Competition, the Cyber Quest Challenges for college students and adults, and the DoD DC3 Digital Challenge by inviting high schools and colleges across Texas to join in and encourage communities to support them with volunteer mentors, instructional clinics, recognition programs, and grants.

The promotion of these programs could lead to the creation of a Texas Digital Challenge with state-level recognition and eventually to national participation in cybersecurity competitions such as the National Collegiate Cyber Defense Competition and the International Capture the Flag event.

BETS can also foster partnerships between education and industry that would lead to internship programs that help develop skilled graduates in cybersecurity fields, mentorship programs, and collaborative research and establish employee training programs in cybersecurity areas.

To provide an incentive to enter the Texas Cybersecurity Education Pipeline, the BETS group might explore creation of a Texas version of the federal Scholarship for Service (SFS) program which provides tuition and support for individuals in cybersecurity-related programs. Alternatively, or additionally, a loan forgiveness program for students should also be explored.

To increase cybersecurity awareness in Texas, the Council recommends that DIR's role be reviewed and sharpened so that DIR can take a leadership role in establishing a sustainable Cybersecurity Awareness Program for all Texans. Not only are national security and economic data at risk, the personal safety and wealth of individual Texans are also at risk, unless Texans' general cybersecurity awareness is enhanced sufficiently to protect them from increasingly sophisticated social engineering and other cybersecurity exploits. DIR should be provided appropriate resources and authority and should work with the Texas Coordinator of Cybersecurity (proposed in the Infrastructure section). Where feasible, DIR could also leverage work already done by other agencies such as the Texas Attorney General's Identity Protection initiative and other established cybersecurity awareness programs in state agencies and higher education. These education and awareness efforts should include programs targeted toward legislators and key stakeholders at all levels of government that are in a position to influence cybersecurity awareness program adoption for their constituencies.

Education Summary

The Council repeatedly noted the need for a trained workforce as it studied cybersecurity issues in Texas. While Texas has much going for it, such as the number of university centers of excellence in cybersecurity, much more must still be accomplished. This is especially true when education is viewed more broadly, as it must be in cybersecurity, and extends beyond formal degree-granting programs to include the Texas citizens who are responsible for securing their own systems and networks.

The ultimate goals of cybersecurity education in Texas would be to provide a well-trained workforce of cybersecurity practitioners steeped in a “Culture of Security” and to create a “Culture of Security Awareness” among all Texans.

Next Steps

During the 1980s, SEMATECH was formed in Austin to support the national security needs of the nation by acting as a hub for shared research and development in the non-competitive domain of semiconductor manufacturing. Today, a similar opportunity exists to form an organization focused on computer, software, network, and human systems related to cybersecurity.

The Council believes that it is important that Texas takes some immediate steps in order to address the issues raised in this report. The first step, which can be accomplished in the first half of 2013 is:

- Through Executive Order, establish a “Business Executives for Texas Security” (BETS) partnership.

This recommendation can be completed without the need for additional funding or legislative approval. It can be accomplished by the Office of the Governor and would not only demonstrate Texas’ commitment to enhancing cybersecurity in the state but also would set the stage for addressing additional recommendations. While BETS can be established in the first half of the year, it will take additional time to select the membership and begin discussions. The goal should be to have a first meeting in the second half of 2013.

During the 83rd Texas legislature, additional steps can be taken to implement the recommendations made by the Council. These next steps will require legislative action and include:

- Establishing a Texas Coordinator of Cybersecurity within the Office of the Governor.
- Empowering DIR to lead implementation of state infrastructure improvement activities in coordination with the Texas Coordinator of Cybersecurity.
- Funding implementation of a program to institute the Community Cyber Security Maturity Model in communities throughout Texas.

Accomplishing these steps in 2013 will provide the leadership necessary to advance Texas’ cybersecurity agenda. Once the Texas Coordinator of Cybersecurity within the Office of the Governor is selected, the individual should quickly meet with BETS in order to continue and advance efforts through 2014 and beyond. At that point, additional steps can be taken to advance the cybersecurity agenda in the state including:

- Utilizing BETS to define a roadmap to improve cybersecurity for key critical infrastructure and industry in the state and increase additional cyber technology investment sources.
- Under DIR leadership, developing a sustainable cybersecurity awareness program for all Texans.

When discussing cybersecurity and industry, the Council noted that BETS must address two issues. The first is the growth of the cybersecurity industry within the state. Cities such as San Antonio have a robust cybersecurity industry which other technology corridors within the state could follow. The second aspect that cybersecurity and industry need to be examined from is “cybersecurity within industry.” This differs from the first in that all industries, regardless of focus, must be concerned with cybersecurity. Cultivating a culture of security within communities and throughout Texas in

which all individuals and organizations are concerned with cybersecurity will help to advance the state's overall posture of cybersecurity. The Council believes that this in itself could become a marketable commodity that could be used not only to attract additional cybersecurity industry to Texas but could also result in an overall increased attraction of industry in general to Texas. The idea is to build on the premise that the strong cybersecurity culture in Texas is such that cyber incidents would be less likely to occur; when they do occur, it is more likely that a coordinated response to the incident will take place, resulting in lower impact to the affected organization.

Following these steps in 2014 will allow the appropriate organizations to address all of the recommendations in this report without a need for the Council to continue as currently tasked. However, as cybersecurity is an ever-changing issue, the Council believes that it might be useful to form another council with a similar charter in 2015 to report on the state's progress and to make necessary adjustments based on either technological or economic factors that may have changed.

Conclusion

There is no question that every day millions of people entrust entities within the State of Texas with personal, financial, and other sensitive information requiring protection at the highest levels. Millions more rely on critical infrastructure networks within the state for basic life needs such as power, water, emergency response, and others. However, as society's reliance on technology continues to increase, so do the ramifications of successful attacks on our technology infrastructures. Sadly, the daily news headlines are full of information security breaches and other results of cyber malfeasance throughout the world.

The good news for Texas is that, through the information gathering conducted during the course of working on this report, the Council found that Texas already has strengths across a spectrum of areas critical to successful cybersecurity efforts. From legislative mandates requiring state agencies to implement basic levels of cybersecurity (such as those found in Texas Administrative Code 202), to multiple Centers of Academic Excellence in Information Assurance, to successful models of metro-area participation in cybersecurity programs and innovation centers, these strengths encompass multiple levels of Texas government, geographic diversity, and public/private collaborations.

What the Council found missing is the framework necessary to collaboratively tie these cybersecurity strengths together. Texas is not alone in this regard. States throughout the nation are struggling to identify successful strategies for addressing cybersecurity concerns.

In crafting the recommendations contained in this report, the Council worked diligently to address the state's challenges while building on its strengths and adhering to the legislative mandate to utilize existing resources. The resulting framework recommendations are both innovative in their approach and straightforward in their purpose. The success of framework implementation will depend on the commitment of the stakeholders in making cybersecurity a priority initiative for Texas. This is especially true in light of recognizing that failure to act on the cybersecurity threat now could adversely impact other key focus areas, such as energy security and border security, for the state.

The benefits of implementing a framework such as recommended in this report extend beyond cybersecurity concerns, and have the ability to improve the well-being of the state in a variety of ways. Increased economic development as a result of these efforts is, of course, a key benefit affecting all Texas citizens. However, it is not the only one. For example, one of the key challenges the Council faced in our information gathering was the act of distributing the public sector survey. While many organizations were identified to participate, efforts to communicate with the organizations proved to be difficult. The establishment of formal communication and collaboration channels among diverse Texas organizations (including municipalities, public and private organizations, and educational institutions) can serve to identify and enhance a wide-range of initiatives throughout Texas.

To be clear, Texas is in a unique position not only to implement a gold-standard level of protection of the state's information assets, but also to become a nationwide leader in cybersecurity that other states can emulate. It is the Council's intention that the recommendations provided in this report will provide the necessary roadmap for the state to achieve the goals of "Building a Secure and More Prosperous Texas." With an increasingly advanced and multi-dimensional threat growing in cyberspace, failure to take comprehensive action now puts all Texas institutions and citizens at significant risk.

Now is the time for Texas to lead. ★

Acknowledgements

The Council would like to thank the following individuals and organizations for their assistance in the creation of this report:

- Dr. John Frederick, Provost, The University of Texas at San Antonio
- Bobby R. Inman, Admiral, U. S. Navy, (Ret.)
- Mark Weatherford, Deputy Under Secretary, U.S. Department of Homeland Security

- AT&T
- CSIdentity (CSID)
- James A. Baker III Institute for Public Policy, Rice University
- Federal Bureau of Investigation
- Gartner, Inc.
- The Greater San Antonio Chamber of Commerce
- National Security Agency
- National White Collar Crime Center
- Texas Army National Guard
- Texas Statewide Information Security Advisory Committee (SISAC)
- USAA
- Valero

In addition to those listed above, through our information gathering efforts the Council received information and feedback from a multitude of organizations and citizens throughout Texas. This information was invaluable in the formulation of our recommendations and this report, and we recognize the contributions of all who assisted us in these efforts. The Council also thanks Vivian Cullipher, Publications Specialist at the Texas Department of Information Resources, for her editing and production contributions.

Appendix A

SB 988 Tasking

The Texas Cybersecurity, Education, and Economic Development Council was created by Senate Bill 988, included below:

A BILL TO BE ENTITLED
AN ACT

relating to the creation of a cybersecurity, education, and economic development council.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Chapter 2054, Government Code, is amended by adding Subchapter N to read as follows:

SUBCHAPTER N. CYBERSECURITY, EDUCATION,
AND ECONOMIC DEVELOPMENT COUNCIL

Sec. 2054.501. DEFINITION. In this subchapter, "council" means the Cybersecurity, Education, and Economic Development Council.

Sec. 2054.502. CYBERSECURITY, EDUCATION, AND ECONOMIC DEVELOPMENT COUNCIL; COMPOSITION. (a) The Cybersecurity, Education, and Economic Development Council is established.

(b) The council is composed of nine members appointed by the executive director. The members must include:

(1) one representative from the department;
(2) one representative from the Texas Economic Development and Tourism Office in the office of the governor;
(3) two representatives from institutions of higher education with cybersecurity-related programs;
(4) one representative from a public junior college, as defined by Section 61.003, Education Code, with a cybersecurity-related program;
(5) one state military forces liaison experienced in the cybersecurity field; and
(6) three representatives from chamber of commerce organizations or businesses who have a cybersecurity background.

(c) The council shall elect a presiding officer from among its members.

(d) A council member serves at the pleasure of the executive director.

Sec. 2054.503. COMPENSATION. A council member serves without compensation or reimbursement of expenses.

Sec. 2054.504. COUNCIL POWERS AND DUTIES. (a) The council shall:

(1) at least quarterly, meet at the call of the presiding officer; and
(2) conduct an interim study and make recommendations to the executive director regarding:

(A) improving the infrastructure of this state's cybersecurity operations with existing resources and through partnerships between government, business, and institutions of higher education; and
(B) examining specific actions to accelerate the growth of cybersecurity as an industry in this state.

(b) The council may request the assistance of state agencies, departments, or offices to carry out its duties.

Sec. 2054.505. REPORT. Not later than December 1, 2012, the council shall submit a report based on its findings to:

(1) the executive director;
(2) the governor;

(3) the lieutenant governor;
(4) the speaker of the house of representatives;
(5) the higher education committees of the senate and
house of representatives;
(6) the Senate Committee on Economic Development;
(7) the House Technology Committee; and
(8) the House Economic and Small Business Development
Committee.

Sec. 2054.506. EXPIRATION OF SUBCHAPTER. This subchapter
expires and the council is abolished September 1, 2013.

SECTION 2. Not later than the 30th day after the effective date of this Act, the executive director of the Department of Information Resources shall appoint the members of the Cybersecurity, Education, and Economic Development Council as established by Subchapter N, Chapter 2054, Government Code, as added by this Act.

SECTION 3. This Act takes effect September 1, 2011.

Appendix B

Council Membership

Council Members	
Robert Butler , Chair	Chief Security Officer/Senior Vice President, IO
Dr. Gregory White , Vice-Chair	Director, Center for Infrastructure Assurance and Security, The University of Texas at San Antonio
Dr. David A. Abarca , CISSP	Asst. Professor and Information Security Program Director, Del Mar College
Dr. Frederick Chang	President and Chief Operating Officer, 21CT, Inc.
Angel Cruz 12/2011–current (replaced Todd Kimbriel)	Chief Information Security Officer, Department of Information Resources
Mary Dickerson , CISSP	Executive Director of IT Security and Chief Information Security Officer, University of Houston/University of Houston System
B. Keith Graf 09/2012–current (replaced Jonathan Taylor)	Director, Aerospace, Aviation, and Defense, & Texas Military Preparedness
Todd Kimbriel 10/2011–12/2011	Director of E-Government, Department of Information Resources (DIR)
Sam Segran , GIAC-GSLC	Chief Information Officer, Texas Tech University
Col. Timothy M. Smith , CISSP	Chief Information Officer, Texas Army National Guard
Jonathan Taylor 10/2011–09/2012	Director, Texas Emerging Technology Fund

<i>Ex Officio</i> Council Members	
Karen Robinson	State of Texas Chief Information Officer Executive Director, Texas Department of Information Resources
Carl Marsh	Chief Operations Officer, Texas Department of Information Resources
Lori Person	Chief Administrative Officer, Texas Department of Information Resources
Martin Zelinsky	General Counsel, Texas Department of Information Resources
Chandra Thompson	Secretariat, Texas Department of Information Resources

Appendix C

Glossary

In the report, a number of terms were used which may have a different meaning to individuals with different backgrounds. For the purpose of this report, the following terms and how they are used in the report are as follows:

Botnet: Derived from the terms “robot” and “network,” a botnet is a network of private computers that are infected with malicious software and controlled as a group by a malicious person or party. Computers are infected without the computer owner’s awareness to automatically send out “Spam” email messages, spread viruses, attack computers and servers, and commit other kinds of cybercrime and fraud.

Credentials: A type of identity data used in a computer system to confirm the identity and authenticate the approved level of access of a given user; most often associated with User ID and Password, but may also use SmartCard and PIN, biometrics, or a set of personal questions that the user must answer.

COGs: Councils of Government

Cyber: Of, relating to, or involving computers or computer networks.

Cyber-attack: A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

CyberPatriot: A high school cyber defense competition run by the Air Force Association which encourages high school students to learn more about cybersecurity through a hands-on competition environment. More can be learned about the program by visiting the CyberPatriot website at www.cyberpatriot.org.

Cyber Quest Challenges: The challenges are a series of on-line competitions which have been designed to challenge participants in a variety of different information security related tests. More information can be found on the challenges at <http://uscc.cyberquests.org>.

Cybersecurity: Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack; also the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

Cybersecurity as an industry: means any business entity that creates and markets security products and services and can also include any company with significant cybersecurity requirements or needs based on their business functions or processes.

Cybersecurity business: Public and private companies who create and market security products and services, and technology companies with significant cybersecurity process capabilities.

Cybersecurity infrastructure: The data centers, networks, servers, computing and telecommunications devices, end users, and controls that protect and support electricity generation, transmission and distribution; gas production, transport and distribution; oil and oil products production, transport and distribution; telecommunication; water supply (drinking water, waste water/sewage, surface water); agriculture, food production and distribution; heating (e.g. natural gas, fuel oil, district heating); public health (hospitals, ambulances); transportation systems (fuel supply, railways, airports, harbors, inland shipping); financial services (banking, clearing); security services (police, military).

Cybersecurity operations: means administrative and technical measures taken to protect the state against unauthorized access or attack, including preventing against criminal or unauthorized use of electronic data.

Data breach: The intentional or unintentional release of secure information to an untrusted environment.

DC3 Forensics Challenge: A cybersecurity competition focusing on digital forensics sponsored by the DoD Cyber Crime Center. The competition is open to individuals or teams from high school through post-higher education levels. More information can be found at their website at www.dc3.mil/challenge.

InfraGard: InfraGard (www.infragard.net) is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

ISP: Internet Service Provider. Any one of many organizations that are community-owned, non-profit, privately owned, or for-profit and provide access to the Internet.

Malware: Short for “*malicious software*.” Refers to a variety of hostile or intrusive software created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems (i.e., viruses, worms, Trojan horses, spyware, adware, etc.).

NCCDC: The National Collegiate Cyber Defense Competition (NCCDC) is the largest collegiate cyber defense competition. It consists of several rounds of competition throughout the nation leading to the national championship held in San Antonio every year. It is only open to college teams though both 2-year and 4-year institutions may participate and even allows a small number of graduate students per team. More information can be found at their website at www.nationalccdc.org.

Phishing: The act of attempting to acquire private information, such as user names, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication; an example of social engineering techniques used to deceive users and exploit the poor usability of current web security technologies.

TDEM: Texas Division of Emergency Management (previously “GDEM,” or “Governor’s Division of Emergency Management”). Operated within the Texas Department of Public Safety, TDEM implements programs to increase public awareness about threats and hazards, coordinates emergency planning, provides an extensive array of specialized training for emergency responders and local officials, and administers disaster recovery and hazard mitigation programs in the State of Texas. See www.txdps.state.tx.us/dem/about.htm for more information.

Business Executives for Texas Security (BETS) Concept

Background and Purpose

- Texas critical infrastructure and security are at increasing risk to both physical and cyber threats. The commercial technology market and the exploitation of this market by nations, terrorists and criminal groups are evolving in ways that present serious risk to the security of Texas infrastructure and Texans. A closer dialogue with Texas industry leaders is needed to create an enabling and enduring framework for addressing today's security risks to Texas and creating a forum for continued engagement in today's technology marketplace.
- The Texas Legislature, in conjunction with the Office of the Governor, has recognized this risk and passed Senate Bill 988 in 2011, establishing a new Texas Cybersecurity, Education and Economic Development Council (Council) to address this risk.
- Recognizing the need for all of Texas' leaders to come together to address this risk, the Council strongly recommends the formation of a new public-private sector partnership, led by the Office of the Governor, with participation from key Executive branch members, key legislators and Texas "industry captains."

Organization and Structure

The Council proposes the following organization and structure for the new Business Executives for Texas Security (BETS) partnership.

- The Texas Legislature shall ensure statute is in place to support the stand-up of BETS, enabling liability protection for company leaders that are selected to participate and government guidance to prevent unfair business practices and full participation by Government members.
- The Governor shall establish an Executive Steering Group (ESG) of key Government leaders and private sector leaders in Texas as the core of the BETS partnership.
 - Government leaders will include, but are not limited to the Lieutenant Governor, Speaker of the House, Attorney General, Chief Information Officer, and Legislature Chairs of related oversight committees, including those pertaining to science, technology, and economic development.
 - Private sector leaders will include no less than six and no more than ten CEOs from Texas critical infrastructure companies to include telecommunications, information technology, energy, transportation and financial services. The Office of the Governor, in conjunction with BETS Legislative leads, may select industry leads.
 - Leaders from other Texas non-profit organizations will include no less than two and no more than four members.

- The BETS partnership should include a senior representative from the Higher Education Coordinating Board (THECB) and from the Texas Education Agency (TEA). Subsequent working groups could leverage expertise from the Education community and other agencies as appropriate.
- The Governor shall select an industry co-chair who can help the Office of the Governor set the agenda for the BETS partnership.
- The BETS partnership will also have an Operations Working Group, co-chaired by a member of the Office of the Governor and an industry co-chair at the SVP level. The Operations Working Group, under the guidance of the ESG, shall be the BETS arm responsible for executing the ESG agenda, convening Subject Matter Experts and “solutioning” to improve Texas’ security posture in the state.
- The BETS partnership, at the ESG level, shall meet at least twice a year and can meet more frequently at the direction of the Office of the Governor and the industry co-chair. The Operations Working Group shall meet as frequently as required to execute the ESG agenda.

Cyber Star Program

General Concept

Similar to the U.S. Environmental Protection Agency's ENERGY STAR program, a Texas Cyber Star program is envisioned as a joint program developed and championed by both public and private sectors (ideally by Business Executives for Texas Security or BETS) to encourage voluntary participation by public and private organizations and aimed at validating that applicants:

- Have a program to keep its workforce educated and aware of the importance of cybersecurity
- Use generally accepted cybersecurity best practices and processes
- Conform with national standards relative to cybersecurity
- Perform regular internal and external assessments of their cybersecurity program
- Demonstrate that they use appropriate and secure technology in their business and/or processes

Objective

The intent of this program is to increase general cybersecurity confidence, both on the part of the public and private organizations who chose to participate in an effort to improve their own e-business environments, as well as among the members of the general public who are customers and clients of those organizations.

Key Suggestions

- Give the private sector the lead in developing this program, including establishing participation criteria, in partnership with the public sector through the BETS organization.
- Limit DIR's role in establishing and promulgating standards or certification requirements for the program to no more than that of any other BETS participant.
- It may be worth considering a model where companies could self-certify either by conducting their own internal audits or contracting with a third party.
- Give consideration to possible incentives (i.e., public/private prize regime) in which Texas-based companies sponsor prizes based on exceptional performers in various categories.
- Leave BETS as much implementation leeway as possible to make the program inviting to the private sector.
- Develop a distinctive certification logo that participants can display.

Community Cyber Security Maturity Model

Excerpted from “A Grassroots Cyber Security Program to Protect the Nation” by Gregory B. White, Ph.D., in the Proceedings of the 45th Hawaii International Conference on System Sciences – 2012

1. Introduction

Many lessons were learned from responding to the attacks of September 11, 2001. This was an event that affected the nation and ultimately had a global impact. While the U.S. federal government was attempting to deal with the impact of the attacks, one lesson that was being learned was that while the event was an attack on the nation, it was the local first responders that had to deal with the immediate effects of the attack. Since that time the nation has spent a considerable amount of money improving the ability of local and state governments and their first responders to deal with an attack of this nature. The lessons that have been learned by the first responder community are equally applicable to the cyber security community. A critical lesson to learn is that while there are numerous cyber events that might have a national level impact, they will also have an impact on state and local entities and local government leaders and cyber first responders need to be prepared to address cyber events that may occur which will have a negative impact on the community.

This paper examines several cyber incidents that have occurred at the local and state levels that illustrate how communities are increasingly becoming reliant upon the various cyber infrastructures and how a cyber event can have a negative impact on the community. This leads to the obvious conclusion that something must be done and the paper introduces a model to help

communities develop viable and sustainable cyber security programs. The implementation of this model is discussed and results based on feedback from state and local officials are presented.

2. Threats to Communities

There are many benefits and reasons for introducing electronic-government at the local level. Governments see increased access, convenience, customer support, lower costs, and more access to information as reasons to increasingly rely on computer systems and networks to provide services to their citizens. [1] While all of these are benefits, the increased reliance on networks, and in particular the Internet, introduces a potential weakness as any of a variety of cyber security events can impact the delivery of the services. There are numerous examples of government entities at various levels experiencing a problem.

In February, 2009 a virus infected almost 500 of the city of Houston’s computer systems. [2] The infection caused the city to shut down part of its municipal courts system including suspending arrests for minor offenses. In addition, the Houston Emergency Center was forced to disconnect from the city network for several hours and forced 3000 people to have their court appearances rescheduled. [3]

While it could be argued that the impact of this incident was minimal – only affecting 3000 citizens already in the system plus

allowing a small number of individuals who had committed minor infractions to avoid arrest – other incidents had considerably greater impact. In April, 2009, a fiber optic cable was deliberately cut in several locations in Silicon Valley. This resulted in loss of 911 access for thousands of customers. [4] In addition, tens of thousands of citizens found they had lost Internet access as well as landline and wireless phone service. [5] The loss of 911 service is obviously critical to a community. An example of another potentially significant issue is the security of electronic voting systems. There has been quite a few studies on this subject, including one event in 2010 in which the Washington D.C. election board invited groups or individuals to attempt to break into the city’s voting system. One group was soon successful in gaining sufficient control to be able to both view and change votes. [6] While this was a public test, it is easy to imagine the potential implications had this flaw not been exposed at that time.

Other incidents illustrate additional events that threaten governments at various levels. In May, 2011, MSNBC posted a story regarding a security researcher penetrating the computer inside a police cruiser. The level of access obtained allowed the researcher to compromise telnet and ftp services as well as to view the current feed from the car’s camera and its stored videos. [7] In another well publicized incident, the state of Virginia was the target of an extortion attempt by an attacker who claimed to have broken into a patient database and then encrypted millions of records maintained by the Virginia health agency. [8] The attacker, who also claimed to have deleted the original file, demanded a \$10 million ransom for the password that would decrypt the file. Since every state and

community will likely have multiple files or databases with sensitive information about its citizens, this incident illustrates the potential harm that might occur should sufficient security not be provided. It also shows that there are individuals that are willing to target states and communities and to attempt to extort money from them.

The types of issues seen in these examples are not confined to the United States. In July, 2010, the website of the Mumbai Cyber Crime Cell was hacked, embarrassing the cyber crime department of the city’s law enforcement agency. [10] The group claiming responsibility for the hack also claimed to have “tampered with the information about most wanted criminals, which included some suspected terrorists.” [10] In another incident in Queensland Australia, a disgruntled individual attacked the computer control systems that managed the city’s wastewater. He was able on numerous occasions to divert the flow so that as much as 1 million liters of raw sewage was dumped onto the grounds of parks, waterways, and a local tourist resort. [11] All of these examples serve to show how the various cyber systems, networks used in the daily operation of the various critical infrastructures in a community, can be attacked and cause mild to severe disruptions in the community. In order to address this, communities need to establish their own cyber security programs and cyber incident handling processes and procedures. Unfortunately, very few communities have such programs and in fact few even have an idea of where to begin.

3. Initial Efforts to Establish Programs

After the physical attacks that occurred September 11, 2001, many state and local governments placed an increased emphasis

on preparing to deal with terrorist attacks using any of the traditional weapons of mass destruction. No real effort, however, was placed on cyber security at the local level. At the national level, discussions were widely held regarding the possibility of a cyber terrorist attack. Efforts were under way at various federal agencies to determine ways to secure the national cyber infrastructures. These efforts were focused on cyber events that would impact the entire nation (or a major portion of it) and involved discussions on how the various federal agencies would interact with industry to address the incident and work toward a resolution. Industry was recognized as a key component of a national response because the majority of the Internet was under the control of industry and not the government. State governments were only minimally considered – basically through the establishment of the Multi-State Information Sharing and Analysis Center (MS-ISAC). No efforts were undertaken to help prepare local governments to address a cyber incident. The problem with this was twofold. First, as has been discussed, should a national cyber event occur, just like the events of 9/11, it is a national incident but state and local officials will be impacted and will need to be able to handle their response to it. Second, a national strategy that doesn't include a state and local piece completely ignores the possibility of an incident that would have only a local impact.

The Center for Infrastructure Assurance and Security (CIAS) decided to address this gap in the plan to secure the nations cyber infrastructures by creating a grass-roots level program that would help secure computer systems and networks at the local and state level, coordinating with federal agencies when appropriate. The first step in this effort

was the creation of a community cyber security exercise for the city of San Antonio. Called Dark Screen, this exercise was conducted in September, 2002 and involved over 200 participants in a tabletop format. The event was a success in terms of making various leaders in the community aware of the potential for disruption that a cyber incident could cause. The participants included not just local city and county government leadership, but members from local utilities, federal agency representatives, and industry. All were made aware of the need to share information and to work together in the event of a cyber incident. As a result of the success of this event, the CIAS obtained funding to conduct similar events in other cities around the country. This occurred from 2003 through 2005.

At each community that the CIAS delivered an exercise in, the event seemed very successful in making the leadership aware of the potential problems a cyber incident would cause. After moving on to the next city, no further work was conducted with the city after the after action report was delivered. After two years, the CIAS began to take a look at the communities in which exercises had previously been conducted. What was discovered was that while the individuals in the community were aware that cyber incidents could be an issue, the communities had not taken any real step toward establishing a cyber security program. The cities were aware of the issues posed by cyber incidents, but they didn't know what to do in order to secure their own critical cyber infrastructures. This was not what had been expected and the CIAS determined that a new approach was needed.

LEVEL 1 Initial	LEVEL 2 Advanced	LEVEL 3 Self-Assessed	LEVEL 4 Integrated	LEVEL 5 Vanguard
<ul style="list-style-type: none"> Minimal cyber awareness Minimal cyber info sharing Minimal cyber assessments and policy & procedure evaluations Little inclusion of cyber into Continuity of Operations Plan (COOP) 	<ul style="list-style-type: none"> Leadership aware of cyber threats, issues and imperatives for cyber security and community cooperative cyber training Informal info sharing/communication in community; working groups established; ad-hoc analysis, little fusion or metrics; professional orgs established or engaged No assessments, but aware of requirement; initial evaluation of policies & procedures Aware of need to integrate cyber security into COOP 	<ul style="list-style-type: none"> Leaders promote org security awareness; formal community cooperative training Formal local info sharing/cyber analysis. initial cyber-physical fusion; informal external info sharing/ cyber analysis and metrics gathering Autonomous tabletop cyber exercises with assessments of info sharing, policies & procedures, and fusion; routine audit program; mentor externals on policies & procedures, auditing and training Include cyber in COOP; formal cyber incident response/recovery 	<ul style="list-style-type: none"> Leaders and orgs promote awareness; citizens aware of cyber security issues Formal info sharing/analysis, internal and external to community; formal local fusion and metrics, initial external efforts Autonomous cyber exercises with assessments of formal info sharing/local fusion; exercises involve live play/metrics assessments Integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery 	<ul style="list-style-type: none"> Awareness a business imperative Fully integrated fusion /analysis center, combining all-source physical and cyber info; create and disseminate near real world picture Accomplish full-scale blended exercises and assess complete fusion capability; involve/mentor other communities/entities Continue to integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery

Figure F-1: The Community Cyber Security Model

4. Development of the CCSMM

The problem in the communities was that the leaders were still aware that a cyber incident could have a negative impact on the community, but they didn't know what to do in order to prepare for one or to address one should it occur. The first attempt to address this was to develop a course that would be provided to the community before the exercise. After the exercise, it was decided to provide some hands-on assistance to communities so that issues raised during the exercise could be addressed. These two additional events proved to be a tremendous step forward in helping communities as it helped them better understand what was needed. These two additions, however, were not enough as communities really needed a roadmap that they could follow to be able to build a viable and sustainable cyber security

program. As a result, CIAS researchers came together and created the Community Cyber Security Maturity Model (CCSMM) to address this need. The model, as shown in Figure F-1, was designed to accomplish three things:

- Serve as a yardstick so that communities can determine where in the model they currently are (i.e. how mature their security program is)
- Serve as a roadmap so that a community knows what it needs to do in order to advance to the next level of the model.
- Provide a common point of reference so that different communities can discuss their respective programs and plans from a common perspective.

The model as shown describes the characteristics of communities at five levels of maturity. The first level basically describes a community that has not established cyber

security program. Unfortunately, in the experience of the CIAS, this has been the level that all communities are at. The next level, “advanced”, describes a program that has advanced in its processes and has established the basics for a continued program. While the characteristics described at this level do not seem extremely difficult to attain, a community displaying all of these characteristics has actually taken a very large step toward establishing a cyber security program. The subsequent levels each build upon the basic characteristics as depicted here until at level 5, a community not only has a mature program but is also serving as an example and helping other communities attempting to establish their own programs. After several years of working with communities, it has been shown that it is possible for communities to establish programs based upon the model, but it will take years for a community to attain level 5.

One axis of the model shows the different levels a community can attain. The other axis describes what a community should have implemented in each of four characteristics. The first of these is awareness and describes how widespread the understanding of what the impact of a cyber incident might be on the community. The second is information sharing which describes what mechanisms are in place within the community to share information about and analyze cyber security events and what fusion efforts are performed to tie disparate pieces of information into a unified threat picture. The third characteristic describes what processes and procedures are in place in various organizations within the community to address cyber security. It also addresses what testing/exercise/practice is accomplished to evaluate the procedures that

have been developed. The final characteristic describes to what extent cyber security is considered in the community’s disaster planning process and what incident response steps have been implemented to cover a cyber incident.

5. Expansion of the CCSMM

The initial model developed was a tremendous first step in developing an approach to help communities establish viable and sustainable cyber security programs. Unfortunately, it soon became obvious that something was still missing. The main problem was that it was quickly realized that for a community to be mature enough in its program to reach the higher levels of the model would require a certain maturity for organizations within the community. In other words, for the community to be secure, the individual organizations within the community needed to also have a certain level of security. For a community to reach the upper levels of the model, it also needs to be able to rely on entities above it to provide certain assistance and information pre- and post-incident. Thus, for a community to be secure requires that the state also have a certain level of security program maturity. This meant the model was not a two-dimensional model as depicted in the Figure F-1 but should actually be a three dimensional model as shown in Figure F-2. This figure does not depict the intricate dependencies that exist between. Instead, it shows that, just like a community, organizations and states also have multiple levels for their programs. The model’s name was not changed, even though it now encompasses more than just a community, because the focus is still on securing the nation from a community grass roots level.

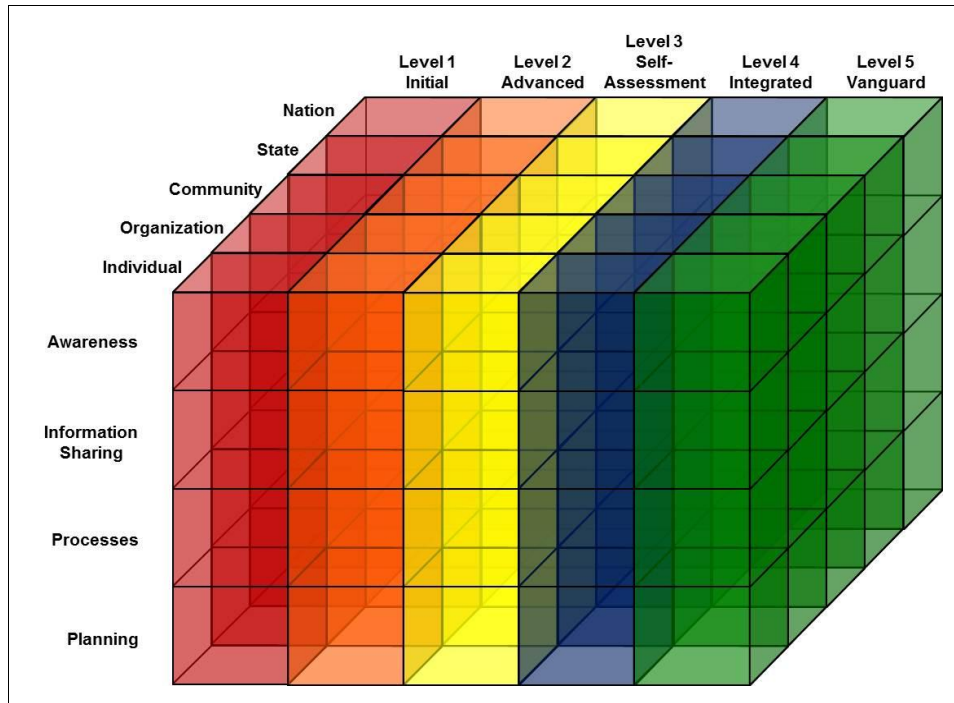


Figure F-2: The expanded 3-D model

While only the three levels of organization, community, and state are shown, other versions of this image include other levels that can be described – namely a national level, an international level, and an individual level. The individual level was a recognition that with the power of computer systems in the home today, individual citizens have a certain responsibility to secure their own systems so that they are not usurped and used, for example, in a distributed denial of service attack. Each of the boxes in the diagram can actually be expanded to describe the different parts of the model that are included at that level. In this image, instead of showing the characteristics at the various levels, the model shows the different parts that are part of a community's program at each level. This includes the metrics that are used to measure the current security posture of the community, the mechanisms that are in place to share information with other entities (whether in the community or upward to the state/nation), the training that is required or

needed for “cyber first responders”, the technology and tools that are needed to accomplish the different tasks that must be performed, the specific processes, procedures, and plans that exist (e.g. an incident response plan), and finally the types of tests and exercises that might be accomplished to evaluate how prepared the community is and how well the responsible “cyber first responders” understand their roles, duties, and responsibilities.

6. Conclusion

The Community Cyber Security Maturity Model, whose implementation has begun in five states within the United States, has shown to be a valuable tool in helping communities take an organized first step in establishing a viable and sustainable cyber security program. The model serves as a yardstick to determine the current level of maturity for a community, a roadmap for the community to follow in order to improve their security program, and a common point of

reference so that individuals in different communities can discuss their individual programs and share experiences and lessons learned. An expanded, three-dimensional version of the model actually illustrates the fact that the model can be expanded beyond the individual community perspective to encompass individual citizens, organizations, the nation, and multiple nations. Results from efforts in the five states the model is currently being implemented in have been very positive and participants in the various events that make up the program to implement the model have indicated that the information they have acquired in the program can be used to help implement programs within their organization and their state.

While much of the model has been developed, there still remain unknowns at the higher levels (since no community is currently at that level). In particular, the technology that will be required to ensure the security of a community in terms of its ability to effectively share information in a timely manner while maintaining the privacy and confidentiality of its citizens and organizations within the community is essential. Without sharing of information, the ability to detect in advance a pending attack will be significantly impacted. The goal should be to prevent attacks from occurring and not just responding to them. This will require a level of information sharing not currently present.

While initial indications are positive, the long-term impact of the program has not been determined since the program is still in its infancy. If communities are not able to sustain momentum then it must be determined what can be done to modify the program to ensure its effectiveness.

7. References

- [1] Oregon.gov, "Oregon E-Government Program Benefits", www.das.state.or.us/DAS/EISPD/EGOV/benefits.shtml, June 14, 2011 .
- [2] SPAMFighter, "Computer Virus Disrupts Houston Municipal Court System", www.spamfighter.com, 13 June 2011.
- [3] Bradley Olson, Melissa Vargas, and Dale Lezon, "Computer virus shuts down Houston municipal courts", Houston Chronicle, Feb 7, 2009, www.abs-comptech.com/home/headlines/news/houston-courts-shut-down-by-malware, 13 June 2011.
- [4] FierceTelecom, "AT&T fiber optic cable cut in California", April 9, 2009, www.fiercetelecom.com, 13 June 2011.
- [5] Malia Wollan, "California" Vandals Cut Phone Cables, Police Say", New York Times online, April 10, 2009, www.nytimes.com, 13 June 2011.
- [6] Mike DeBonis, "Michigan prof explains how D.C. online voting system was updated.", Washingtonpost.com, voices.washingtonpost.com/devonis/2010/10, 13 June 2011.
- [7] Matt Liebowitz, "Cop Car's Computer Hacked by Security Researcher", msnbc.com, 5/30/2011, www.msnbc.msn.com, 13 June 2011.
- [8] Jaikumar Vijayan, "Web site offline as police, FBI investigate extortion bid," IT Health Care, May 7, 2009, www.ithealthcare.computerworld.com, 13 June 2011.
- [9] Lifelock, "Virginia DHP Gets Their Data Held Hostage", May 5, 2009, www.lifelockpromotioncode.net/blog/virginia-dhp-gets-their-data-held-hostage/, 14 June 2011.
- [10] Shalini Desai, "City's cyber crime website hacked.", July 12, 2010, www.mumbaimirror.com, 13 June 2011.
- [11] Todd Datz, "SCADA System Security: Out of Control", csoonline.com, August 1, 2004, www.csoonline.com/article/print/219486, 14 June 2011.

Report Information Gathering Efforts

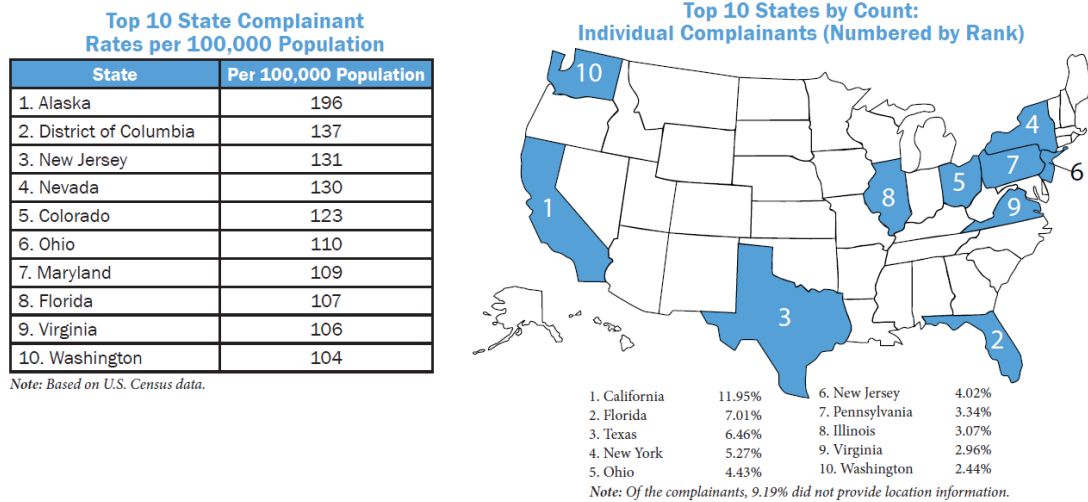
To arrive at a comprehensive understanding of the current cybersecurity environment in Texas, as well as determine consideration for recommendations, the Texas Cybersecurity, Education, and Economic Development Council (Council) utilized multiple approaches for gathering information. The following is a brief summary of the actions taken. Acknowledgement of participation by specific organizations and/or individuals can be found just prior to Appendix A.

- **Public Sector Survey** – The Council created an on-line survey that was distributed to over 5,000 individuals in Texas representing the following organizations: Local, State, Federal Agencies, Military Installations, K–12 School Districts, Higher Education Institutions, Health Science Centers, Hospitals, Ports, Telecommunications, Public Utilities: Electric, Natural Gas, Water, Chambers of Commerce and Emergency Services. The survey questions centered around the organizations’ implementation of cybersecurity education programs and tactical strategy in the areas of people, process, and technology. The goal of the survey was to gauge the overall maturity of cybersecurity programs across the state as well as identify areas of common best practices.
- **Industry Survey** – A phone survey was conducted by Council members with corporate executives at private companies both within and outside of the state of Texas. Questions involved topics such as driving factors for corporate locations, barriers to investment, and cybersecurity concerns.
- **Interactive Dialogues** – Through a variety of face to face meetings, workshops, and seminars in multiple cities throughout Texas, the Council solicited information and feedback on items contained in the recommendations. These discussions addressed not only best practices to be included in the recommendations, but also provided advice on recommendations to be avoided.
- **Subject Matter Experts** – Leveraging the expertise available, the Council engaged cybersecurity experts from federal, state, and local agencies as well as private industry and higher education as a means of fully exploring the areas of recommendations. The experts participated in discussions regarding specific topic areas as well as red-team review of the draft recommendations.

Examples of Cybersecurity Incidents

Among cyber risks and threats to Texas business and their customers are:

- **Loss of Privacy:** Texas has been subject to recently reported or discovered cyber incident events that violated customer privacy. Texas requires appropriate cybersecurity operations capabilities to assure the privacy of customer Social Security Numbers, Driver License Numbers, Credit Card data, private health information, and other personal data. According to the Identity Theft Research Center:
 - Of the 498 nationwide events in 2009 that exposed over 223 million customer records, 28 Texas events impacted nearly 70,000 customers;
 - Of the 662 nationwide events in 2010 that exposed over 16 million customer records, 35 Texas events impacted 140,000 customers;
 - Of the 419 nationwide events in 2011 that exposed nearly 23 million customer records, 31 Texas events impacted 8,780,000 customers;
 - Of the 212 nationwide events from January to June 2012 that improperly exposed over 8.5 million customer records, 13 Texas events impacted 90,000 customers.
- **Internet Crime:** Texas citizens have been subject to recently reported cybercrime events that placed them at risk of identity theft. Texas requires the ability to deliver cybersecurity awareness to Texas citizens of cyber threats to their identities that can cause them long term financial harm, and how they can protect themselves against cyber criminals. In the “2011 Internet Crime Report” produced by the Internet Crime Complaint Center:
 - Texas ranks third with the most individual complainants for being victims of Internet crimes (see Figure H-1 below).
 - While Texas did not appear in the Top 10 states based on per capita complaints, a significant number of Texans (18,477) filed as complainants of Internet crime.



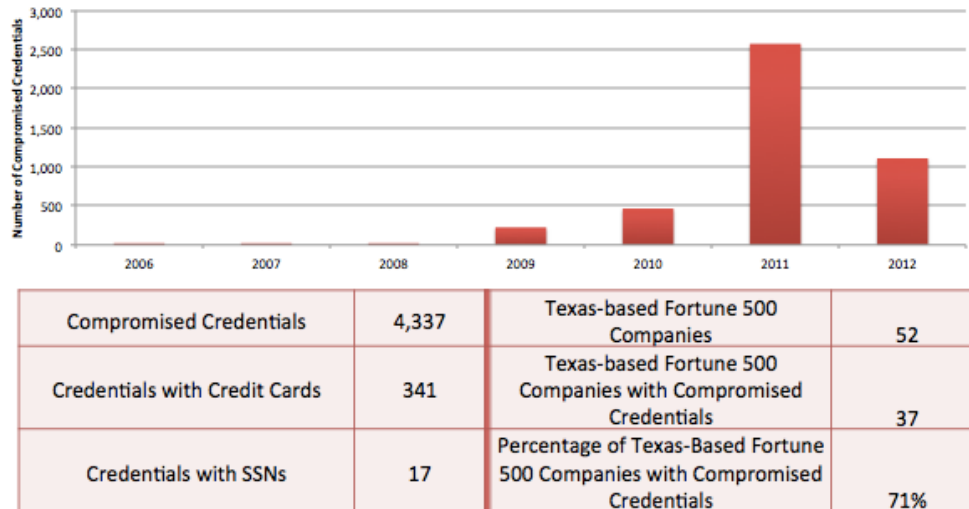
Source: Internet Crime Complaint Center

Figure H-1: Rankings of States in terms of Complaints Regarding Internet Crime

- Intellectual Property Rights:** The Federal Bureau of Investigation has made preventing intellectual property theft a top priority of their cyber program – with a special focus on the theft of trade secrets and infringements on products that can impact consumers’ health and safety. Texas needs an appropriate cybersecurity infrastructure to protect intellectual property belonging to nearly every Texas business organization including product designs and chemical formulae, sales and pricing strategies, strategic plans and financial data, and personnel and customer information. The FBI has noted a significant increase in nation states conducting intellectual property theft activity against U.S. businesses large and small – in fact they report they are “currently working over 400 such cases—many with a global nexus.” The Texas cyber environment has been subject to recently reported cyber espionage events that placed Texas business at financial risk.
 - A former Houston-based Dow Chemical scientist was arrested in 2008 and later convicted for stealing and selling trade secrets worth millions of dollars to China.
 - Two Houston based men who admitted that they manufactured and sold oilfield pipe couplings improperly stamped with the American Petroleum Institute (API) certification mark with many of those couplings made using substandard materials.
 - A U.S. citizen residing in Houston plead guilty to theft of trade secrets in April 2012 and admitted he illegally copied and downloaded intellectual property, specifically product data sheets, belonging to his employer in an effort to economically benefit himself.
- Critical Infrastructure Outages:** The U.S. federal government has recognized that massive power outages caused by cyber events could disrupt the nation’s economy. The U.S. Industrial Control System Cyber Emergency Response Team that monitors control system vulnerabilities notes a significant increase in attempted cyber-attack against U.S. public and private critical

infrastructure companies - nine incident reports in 2009, 41 incident reports in 2010, 198 incident reports in 2011. Texas critical infrastructures support strategic state capabilities such as electricity generation, transmission and distribution; gas production, transport and distribution; oil and oil products production, transport and distribution; telecommunication; water supply (drinking water, waste water/sewage, surface water); agriculture, food production and distribution; heating (e.g. natural gas, fuel oil, district heating); public health (hospitals, ambulances); transportation systems (fuel supply, railways, airports, harbors, inland shipping); financial services (banking, clearing); and security services (police, military). These infrastructures contain many legacy or older systems that cannot be easily replaced or updated to make them more resilient to cyber threats. Some high profile cyber events impacting critical infrastructure include:

- Cyber-attacks that caused power outages in parts of Brazil in January 2005 and September 2007;
 - Over 1 million Texans being impacted by weather related power outages in February 2011;
 - An Iranian natural gas pipeline that exploded and along with a main oil exporting facility, were shut down in 2011 by cyber-attacks;
 - Anonymous computer hacking activists allegedly breaching computer systems of major energy companies including Shell, BP Global, ExxonMobil, Gazprom, and Rosneft in June and July 2012 to protest offshore drilling in the arctic.
 - Power outages in July 2012 leaving 600 million people without power, bank ATMs, or traffic lights, and impacted companies and entities lacking emergency power or other continuity capabilities.
- **Large Corporation Exposure:** Fifty-two Fortune 500 companies operate their headquarters within the state of Texas and hundreds more perform considerable business within the state. A rising corporate threat to large organizations is the exposure – through breach, phishing, or cybercrime – of their employee usernames, passwords, and credentials. Several high profile breach events in 2012 as well as many more that are unreported involved access by a hacker to personally identifiable information and/or financial information that is housed within these organizations:
 - Experian exposure through Texas credit union: Cyber-thieves broke into an Abilene Telco Federal Credit Union employee's computer and stole the password for the bank's online account with Experian plc, the credit reporting agency with data on more than 740 million consumers. The intruders then downloaded credit reports on 847 people, taking Social Security numbers, birthdates and detailed financial data on people across the country who had never done business with Abilene Telco.
 - The number of compromised credentials leaked from Texas-based Fortune 500 companies has increased 395% since 200.



Source: CSID Independent Analysis – 2012

Figure H-2. Compromised Credentials for Texas-based Fortune 500 Companies (2006–2012)

- **Malware and Botnet Operation:** Malware poses one of the most significant threats to individuals and organizations within the State of Texas due to the inherent ability to infect computers at large scale in order to record sensitive information such as keystrokes and screenshots and subsequently exfiltrate that data to a command and control server for harvesting and redistribution. Texas has also been a source for cybertheives hosting botnet command and control servers and propagating malware:
 - The federal government shut down massive Coreflood botnet run out of North Texas and elsewhere, substituting its own servers for criminal's servers to identify victims and send warnings to ISPs.
 - The specific botnet, Coreflood, is a particularly harmful type of malicious software that records keystrokes and private communications on a computer. Once a computer is infected with Coreflood, it can be controlled remotely from another computer. According to information contained in court filings the group of all computers infected with Coreflood is believed to have been operating for nearly a decade and to have infected more than two million computers worldwide.

Appendix I

Resources and References

The Council examined a number of documents in order to draw from the experience of other studies in related areas. These documents provided much insight into the issues surrounding the challenges faced in Texas and a list of some of the more pertinent documents and where they can be obtained follows:

- “Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency”
http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
- “A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency”
http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf
- “Cybersecurity Two Years Later. A Report of the Commission on Cybersecurity for the 44th Presidency”
http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf
- “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure” www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- “Department of Defense Strategy for Operating in Cyberspace”
www.defense.gov/news/d20110714cyber.pdf
- “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.”
www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- “Report of the State Infrastructure Protection Advisory Committee (SIPAC)”
http://staff.washington.edu/dittrich/center/docs/sipac_report.pdf
- “State Enterprise Security Plan: Securing Texas Information Resources”
www2.dir.state.tx.us/SiteCollectionDocuments/Security/Policies and Standards/StateEnterpriseSecurityPlan.pdf
- State of Texas Information and Computer Technology Cluster Assessment
www.texasindustryprofiles.com/PDF/twcClusterReports/TexasITCluster.pdf
- Texas Homeland Security Strategic Plan: 2010–2015
http://governor.state.tx.us/files/homeland/HmLndSecurity_StratPlan2015.pdf

For more about the
Texas Cybersecurity, Education, and Economic Development Council,
please see www.dir.texas.gov/sponsored/sb988/pages/overview.aspx.